ASSEMBLÉE NATIONALE DU QUÉBEC

DEUXIÈME SESSION QUARANTE-DEUXIÈME LÉGISLATURE

Journal des débats

de la Commission permanente des finances publiques

Le mercredi 24 novembre 2021 — Vol. 46 N° 3

Consultations particulières sur le projet de loi n° 6 — Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions (2)

Président de l'Assemblée nationale :
M. François Paradis

2021

Commission des finances publiques

Le mercredi 24 novembre 2021 — Vol. 46 N° 3

Table des matières

Autres intervenants

M. Jean-François Simard, président

M. Éric Caire
Mme Marwah Rizqy
Mme Marie-Claude Nichols
M. Mario Asselin
M. Youri Chassin

* M. José Lemay-Leclerc, Télétravail Québec
* M. Charles Caza, idem

* Témoins interrogés par les membres de la commission

Le mercredi 24 novembre 2021 — Vol. 46 N° 3

Consultations particulières sur le projet de loi n° 6 — Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions (2)

(Quinze heures dix minutes)

Le Président (M. Simard) : Alors, chers collègues, très heureux de vous retrouver. Nous sommes en mesure de reprendre nos auditions.

Comme vous le savez, la commission est réunie afin de poursuivre les consultations particulières et les auditions publiques sur le projet de loi n° 6, Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions.

M. le secrétaire, bonjour. Y aurait-il des remplacements?

Le Secrétaire : Oui, M. le Président. M. Derraji (Nelligan) est remplacé par Mme Rizqy (Saint-Laurent); M. Leitão (Robert-Baldwin) est remplacé par Mme Nichols (Vaudreuil); Mme Ghazal (Mercier) est remplacée par M. Zanetti (Jean-Lesage).

Auditions (suite)

Le Président (M. Simard) : Alors, bienvenue à nos collègues. Cet après-midi, nous entendrons deux groupes, soit Télétravail Québec, les représentants sont d'ailleurs avec nous en ce moment, et, plus tard, nous recevrons M. Steven Lachance. Alors, messieurs, bienvenue parmi nous. Auriez-vous l'amabilité, d'abord, de vous représenter?

Télétravail Québec

M. Lemay-Leclerc (José) : Parfait, merci beaucoup, M. le Président. Donc, mon nom, c'est José Lemay-Leclerc. Je suis président de Télétravail Québec. Avant tout, je suis un expert en informatique. Je suis spécialiste en migration et aussi en implantation infonuagique depuis près de 20 ans. Donc, je viens ici parce que, dans mon expérience, j'ai pu voir plusieurs incidents en cybersécurité, et donc ça m'a amené à m'interposer dans ce beau projet. Je félicite d'abord, là, la mise en place de ce ministère. C'est une très bonne idée, là, de rassembler ces expertises et de voir grand.

Donc, maintenant, pour Télétravail Québec, on est un organisme, depuis 2018, avec plus de 80 membres. Notre mission, c'est d'améliorer les conditions de travail des Québécois en partageant les meilleures pratiques concernant le télétravail. Donc, depuis peu, là, depuis 2020, en septembre, nous avons organisé la Semaine du télétravail. Ce fut un très bel événement, couvrant plusieurs sujets, dont la cybersécurité. Ensuite, les services qu'on offre, là, c'est essentiellement de partager les bonnes pratiques, et aussi on fait de la formation de main-d'oeuvre.

Donc, maintenant, si vous me permettez, M. le Président, je permettrais à mon conseiller de prendre la parole.

M. Caza (Charles) : Bonjour, M. le Président. Charles Caza, je suis conseiller pour Télétravail Québec, mais je suis avant tout avocat et conseiller en relations industrielles agréé. Je suis membre des deux corporations et je suis aussi l'auteur d'un livre sur le télétravail qui a été édité à l'automne 2020. En fait, je suis auteur de plusieurs livres en relations de travail. Je suis conférencier et formateur puis je suis aussi... J'ai été aussi professeur à l'École du Barreau puis aux HEC voilà quelques années. Donc, voilà. Je suis avocat à mon propre compte dans le cabinet Astell Caza.

Le Président (M. Simard) : Alors, soyez les bienvenus, et vous disposez de 10 minutes.

M. Lemay-Leclerc (José) : Parfait, merci beaucoup. Donc, en premier, nous avons une problématique qu'on a remarquée. En fait, c'est en partenariat avec notre partenaire... J'ai consulté Jean-Philippe Racine, qui est président de la firme Groupe Cyberswat. Ce qu'on remarque, c'est que, là, en jumelant la cybersécurité et le numérique, il n'y aura pas d'indépendance réelle entre les deux. Donc, ce qu'il nous explique, là, il nous explique d'avoir une préoccupation à ce sujet et souhaite que les impératifs de livraison du volet numérique n'aient pas le dessus sur le volet cybersécurité.

À titre d'exemple, ce qu'ils font pour les entreprises, c'est qu'ils recommandent toujours de ne pas mettre le service de cybersécurité sous la direction des technologies de l'information car il y aurait un conflit d'intérêts dans la gestion de l'infrastructure TI et la gestion de cybersécurité. Comme il nous dit, là, il est donc primordial que le gouvernement assure une distinction claire entre la TI et la cybersécurité. Qui plus est, il faudrait assurer une séparation étanche entre les deux pour éviter que les intérêts des deux volets s'entremêlent.

Donc, si je passe à une deuxième problématique qu'on a remarquée, en ce qui concerne les réseaux domestiques à des fins commerciales ou d'affaires... En fait, bien, nous, chez Télétravail Québec, on suit de très près les télétravailleurs et on a vu très bien, là, que les travailleurs, en travaillant de la maison, bien, ils utilisent leur réseau domestique à des fins d'affaires ou commerciales.

Donc, on croit qu'il y aurait vraiment place à arriver avec des règles ou des bonnes façons de faire pour limiter le piratage et les vols de données. Ça permettrait vraiment, là, de s'aventurer, je pense, là-dedans et de faire

progresser la chose. On croit, dans le fond, que le gouvernement doit clarifier ses intentions en ce qui concerne le télétravail et surtout comment le tout sera opérationnalisé. Il faut s'assurer que l'utilisation des réseaux domestiques par les fonctionnaires aussi ne viendrait pas créer une brèche en matière de cybersécurité.

Donc, si on passe maintenant à la problématique... à la troisième problématique, c'est en lien avec les réseaux wifi publics, les réseaux publics qu'on utilise dans les commerces ou tout lieu. En fait, ces réseaux, bien, comme ça le dit, c'est des réseaux informatiques. Donc, on branche nos appareils sur ces réseaux-là, et il n'y a pas vraiment de standard de sécurité en place jusqu'à maintenant. Et je pense que ce ministère-là pourrait très bien répondre à ça, arriver avec, peut-être, des normes, des guides afin que les commerces puissent avoir des réseaux qui sont fiables et qu'on ne soit pas victimes, là, de piratage, là, à travers ces réseaux.

Si on passe à la quatrième problématique, c'est concernant les appareils informatiques vendus avec des configurations minimales ou absentes de sécurité. En fait, quand on achète un appareil informatique, si on achète un routeur ou une imprimante, souvent, presque toujours, les configurations d'origine sont presque absentes. Pour se connecter à l'appareil, il n'y a aucun mot de passe qui est requis ou bien c'est un mot de passe qui est très connu, comme «admin» ou «1234».

Donc, ce qui a déjà été fait, en Californie, il y a déjà une loi, qui a été passée en 2020, qui interdit la vente d'appareils non configurés préalablement. Ça, c'est sûr que ça a un grand impact. C'est très connu, là, dans plusieurs statistiques, qu'énormément de piratages sont causés par ces configurations-là qui n'ont soit pas été corrigées dès l'achat, ou soit que les paramètres ont été réinitialisés, et que, là, lors de réinitialisation, le mot de passe par défaut a été appliqué, et là le pirate a pu entrer très facilement. Donc, d'arriver avec une loi comme ça, ça réglerait beaucoup de problèmes, c'est certain.

Puis, si je peux continuer, là, dans un même ordre d'idées, le gouvernement doit statuer si la gestion des appels d'offres en TI demeure comme elle l'est actuellement, soit à la discrétion des ministères et organismes, ou si celle-ci est rapatriée au sein du futur ministère de la Cybersécurité et du Numérique ou même au Centre d'acquisitions gouvernementales. Dans tous les cas, il faudrait s'assurer d'engager le personnel compétent et s'assurer que les appels d'offres en TI respectent le plus haut standard de qualité et de sécurité.

Maintenant, nos recommandations. En résumé, la première est que les parlementaires reconnaissent le conflit d'intérêts et annoncent de quelle façon ils s'assurent que le volet numérique n'aura pas le dessus sur le volet cybersécurité; deuxième, que le gouvernement clarifie ses intentions en ce qui concerne l'implantation du télétravail dans la fonction publique et que les mesures soient mises en place pour ne pas délaisser la cybersécurité; en troisième, que le gouvernement mette en place une politique claire en ce qui concerne l'utilisation de réseaux publics par les fonctionnaires; en quatrième, que le gouvernement mette en place des balises claires avec des mesures coercitives adéquates dans le cadre des appels d'offres en TI et cybersécurité en mettant l'emphase sur la notion d'imputabilité; et, en cinquième, que le gouvernement clarifie l'instance qui sera responsable de piloter les appels d'offres en TI et cybersécurité afin de savoir si ceux-ci sont rapatriés au sein du futur ministère de la Cybersécurité et du Numérique ou au Centre d'acquisitions gouvernementales.

Donc, je vous remercie beaucoup puis je suis disponible pour vos questions.

Le Président (M. Simard) : Merci. M. Caza, souhaitiez-vous, à ce stade-ci, intervenir?

M. Caza (Charles) : Non, pas à ce stade-ci. Merci.

Le Président (M. Simard) : Très bien. Je cède maintenant la parole à M. le ministre.

M. Caire : Oui, bonjour. En fait, je vais avoir quelques questions pour vous, M. Lemay-Leclerc. La première, j'ai trouvé le terme fort puis j'aimerais ça vous entendre là-dessus, parce que vous parlez de conflit d'intérêts entre la cybersécurité et le numérique, alors que, partout ailleurs, je vous dirais, on voit ces deux éléments-là comme étant indissociables. On parle même de «security by design». Dès la conception, on doit avoir... Donc, d'un côté, on a ceux qui disent : Non seulement ce n'est pas un conflit d'intérêts, mais ça doit collaborer à toutes les étapes de la conception, de la réalisation, du déploiement et de l'exploitation, et vous, vous parlez, là, de conflit d'intérêts. J'aimerais ça vous entendre là-dessus, parce qu'honnêtement c'est la première fois que je l'entends, celle-là.

M. Lemay-Leclerc (José) : Bien, en fait, le terme est un petit peu... Peut-être que ce n'est pas le meilleur terme, mais, en fait, c'est surtout que la cybersécurité, en fait, surveille le numérique. Donc, il ne faut pas que ce soit nécessairement les mêmes gens. Il faut que ces gens-là n'aient rien qui les empêche de facilement surveiller, là. Donc, c'est simplement une recommandation qu'on veut s'assurer qu'il n'y a pas de mécanisme qui pourrait protéger ou qui pourrait permettre... Tu sais, je pense qu'on... Dans le fond, il faudrait vraiment que la cybersécurité soit quand même indépendante, même si elle est sous le même ministère.

M. Caire : Mais est-ce que vous adhérez au principe de sécurité à la conception?

M. Lemay-Leclerc (José) : Oui, oui.

M. Caire : Donc, est-ce qu'on peut dire que les experts de sécurité doivent être impliqués à la conception, à la réalisation, à la mise en production, à l'exploitation?

M. Lemay-Leclerc (José) : Ah oui! Oui, bien sûr, à ce niveau-là, c'est très important d'utiliser ces ressources-là, ces expertises-là. C'est vraiment après, pour ce qui est de la surveillance, là...

M. Caire : Si je résume votre pensée, M. Lemay-Leclerc, ce que vous dites, c'est qu'au nom de la réalisation d'applications numériques il ne faut pas faire de compromis sur la sécurité?

M. Lemay-Leclerc (José) : Oui, un peu, oui.

M. Caire : O.K., mais vous ne voyez pas d'objection, au contraire, à ce que ces deux spécialités-là travaillent de concert, là?

M. Lemay-Leclerc (José) : Ah non! Puis c'est même... On l'encourage, là, qu'elles travaillent ensemble.

M. Caire : O.K. Donc, de les réunir au sein d'un même ministère, ça devient une nécessité, dans les faits?

M. Lemay-Leclerc (José) : Oui, tant, quand même, qu'ils peuvent avoir quand même un droit de surveillance, là, sur leurs collègues.

• *(15 h 20)* •

M. Caire : Oui, c'est ça, j'entends ce que vous dites. Dans le fond, c'est... le spécialiste de la cybersécurité devrait toujours avoir le dernier mot.

M. Lemay-Leclerc (José) : Oui, exactement.

M. Caire : O.K., je comprends bien. Bon, sur l'implantation du télétravail, je vous dirais que, sur le normatif, je vais vous dire ce que j'ai répété à différents groupes, évidemment, ça relève de la prérogative du Conseil du trésor d'établir les règles, de discuter de ça avec nos partenaires syndicaux et d'émettre des directives qui vont aller dans le sens de ces consensus-là.

Par contre, là où vous attirez mon attention, c'est quand vous parlez de la sécurité des réseaux. Bon, évidemment, le gouvernement du Québec ne peut pas obliger un individu à utiliser tel, ou tel, ou tel service, mais, quand vous parlez de sécuriser le... À part le réseau... Évidemment, celui du gouvernement, sur lequel on a la mainmise puis, bon, on peut établir les normes, on peut mettre en place tous les applicatifs qu'on veut pour s'assurer de la sécurité des systèmes et des informations, mais, les réseaux domestiques, vous voyez quoi, vous, comme intervention gouvernementale qui va, oui, aller dans le sens de sécuriser le réseau, mais qui va quand même respecter la vie privée des individus? Parce que, là, il y a une notion de vie privée là-dedans. Le gouvernement ne peut pas prendre le contrôle des réseaux utilisés par les individus chez eux.

M. Lemay-Leclerc (José) : Même là, il faudrait faire une grande réflexion là-dessus, peut-être. On pourrait impliquer, je pense, les fournisseurs Internet, les grands fournisseurs, là, qui vont inclure un routeur qui est surveillé par le fournisseur. Ça, c'est déjà un standard un peu mieux que de laisser la liberté au travailleur d'aller chercher son routeur au Bureau en Gros ou un autre commerce, et là, par la suite, il doit lui-même s'occuper de la sécurité de son routeur. S'il peut y avoir des bonnes pratiques de partagées, ça peut être très bien, là. Donc, oui, c'est là-dessus un peu qu'on y va, là.

M. Caire : M. Caza, voulez-vous intervenir, là?

M. Caza (Charles) : Pardon?

M. Caire : Vouliez-vous intervenir? Parce que je voyais qu'il y avait une discussion. Vouliez-vous intervenir, M. Caza?

M. Caza (Charles) : Non, non, c'est parce qu'on m'a demandé d'enlever la bouteille Naya.

M. Caire : O.K., mais parce que le ministère de la Cybersécurité et du Numérique... Tel que rédigé dans la loi, il y a un mandat de cybersécurité qui est donné à ce ministère-là, si l'Assemblée nationale adopte le projet de loi, qui dépasse les frontières de l'État. Donc, vous amenez quelque chose qui est intéressant au niveau des fournisseurs de services. Évidemment, ce ministère-là va pouvoir édicter des normes pour ses propres réseaux. Il va pouvoir suivre des standards pour ses propres réseaux, évidemment, parce qu'au niveau de l'État il ne devrait pas y avoir de compromis sur la cybersécurité et la cyberdéfense.

Maintenant, si je suis votre logique, ces standards-là pourraient s'appliquer aux fournisseurs de services au Québec. Maintenant, est-ce que vous ne craignez pas que ça pourrait avoir un impact sur le prix, donc la disponibilité du réseau, sur la disponibilité des services? Parce qu'on l'a vu dans d'autres dossiers, quand on amène des normes, des standards qui sont plus élevés, évidemment, ça amène des contraintes. Donc, est-ce que, ce faisant, le remède n'est pas pire que la maladie?

M. Lemay-Leclerc (José) : Oui, bien, tu sais, comme je l'ai écrit dans le mémoire, c'est un peu un beau problème, parce qu'en même temps c'est sûr qu'on utilise... On surutilise l'Internet résidentiel. Ça fait que je pense qu'il y aurait quand même place à ce qu'il y ait des forfaits qui ne seraient pas affaires, pas résidentiels, mais peut-être télétravail, et que, là, il y aurait en place ces mesures-là et que, là, au moins, il y aurait une protection additionnelle, là, idéalement, là.

M. Caire : Dans quelle mesure... Puis là je reviens avec mon dada. Dans quelle mesure une certaine littératie numérique, de formation, pour, peut-être, permettre aux gens de mieux comprendre comment ça fonctionne, un réseau, comment on peut le sécuriser, dans quelle mesure, ça, ça ne pourrait pas être une solution peut-être plus démocratique et qui permettrait aux gens, à ce moment-là... Bon, on respecterait la liberté du consommateur, on respecterait la vie privée des individus. Ça ne serait pas intrusif dans leur capacité à choisir tel ou tel ou tel fournisseur. Mais, en même temps, un consommateur éclairé est un meilleur consommateur.

Donc, je m'étonne un peu de ne pas voir cette recommandation-là. Et même chez vos membres, j'imagine, là, que... de voir le gouvernement, là, imposer des standards, je ne sais pas jusqu'à quel point vos membres sont consultés. Puis je ne veux pas présumer de rien, là, comprenez-moi bien, mais jusqu'à quel point cette idée-là serait bien reçue, surtout par des utilisateurs importants, là, d'Internet? Donc, jusqu'à quel point on n'est peut-être pas mieux d'aller du côté de la formation et de l'information en général?

M. Lemay-Leclerc (José) : Oui, c'est sûr qu'on... Dans le fond, la vie privée est vraiment importante pour nous. Ça peut être sous un programme, là, de formation, tout simplement, un partage des bonnes pratiques d'un réseau à la maison. Ça serait quand même une très bonne idée, là, oui, bien d'accord là-dessus.

M. Caire : Parce que, dans le fond, on comprend que ça prend un réseau, là, effectivement, avec un appareil qui, lui-même, n'offre pas des portes dérobées, qui a une bonne sécurité, avec un mot de passe qui est robuste. Puis, bon, on est capables de faire des trucs intéressants, mais encore faut-il bien comprendre comment tout ça fonctionne. Ce n'est pas nécessairement très complexe.

Je vous soumets une idée. Le gouvernement du Québec rend disponible, pour ses employés, quatre formations, sur le site de l'académie de transformation numérique, qui permettent de comprendre... bon, là, on va dans un autre domaine, un peu, que le domaine technique, mais je pense que le parallèle peut être fait, qui permet de bien comprendre la logique des pirates, comment on va se servir des outils informatiques, courriels, textos, pour piéger les gens, comment on peut détecter ces pièges-là, comment on peut évidemment les éviter.

Quelle est la bonne réaction quand on reçoit un courriel litigieux ou un texto litigieux comme j'ai reçu hier, là, où on me disait, là, que ma carte de crédit... un courriel avec aucune... un texto, aucune identification, deux hyperliens, qui nous dit : Votre carte bancaire a été bloquée. Bien oui, aïe, voyons donc, alors... mais, quand on le sait, on rigole, on supprime le texto puis on passe à autre chose, puis, quand on ne le sait pas, malheureusement, on clique.

Donc, jusqu'à quel point, ça, ça pourrait peut-être être une avenue intéressante, de demander à mettre en place ce genre de formation là pour permettre à la population de... aux citoyens qui sont intéressés de peut-être un peu mieux comprendre puis de s'équiper en conséquence?

M. Lemay-Leclerc (José) : Oui, effectivement, c'est sûr qu'avoir ce genre de formation là, là, ça aiderait beaucoup l'éducation, là, des travailleurs, s'assurer qu'ils ont tout en main, là, pour être bien à l'abri, là, de toutes ces fraudes-là, là, oui.

M. Caire : O.K. Là, vous parlez de balises claires avec des mesures coercitives adéquates dans le cadre des appels d'offres en TI, en cybersécurité. Qu'est-ce que vous appelez des mesures coercitives adéquates?

M. Lemay-Leclerc (José) : En fait, ça, c'est pour la dernière ici, ça serait, dans le fond, qu'il y ait... que, dans le fond, les appels d'offres soient vraiment analysés de façon égale, là, entre elles, là.

M. Caire : O.K., mais c'est parce que, si vous dites ça, c'est... J'imagine... En tout cas, je présume, puis j'aimerais vous entendre là-dessus, que vous avez identifié peut-être des lacunes quant à l'évaluation des appels d'offres, parce que, généralement, les appels d'offres, il y a un certain nombre de critères qui valent un certain nombre de points. Ceux qui se qualifient, ils s'en vont à ce qu'on appelle l'ouverture des enveloppes. On regarde le moins cher, puis c'est lui qui a le contrat. Mais, quand vous parlez de mesures coercitives, la coercition, normalement, c'est parce qu'on veut restreindre quelque chose ou carrément l'empêcher. Vous faites référence à quoi? Je vous avoue que, celui-là, je le comprends un peu moins.

M. Lemay-Leclerc (José) : Oui, bien, ça, en gros, c'est vraiment pour que les appels d'offres puissent permettre plusieurs, là, à soumissionner, que ce ne soit pas trop restrictif, là, dans les demandes, là.

• *(15 h 30)* •

M. Caire : O.K., c'est parce que je... O.K., coercitif. Vous parlez d'interdire la vente d'appareils dont les mots de passe par défaut sont trop facilement piratables, mais techniquement, quand on a un mot de passe par défaut, l'appareil va forcer l'acquéreur à le changer à la première utilisation.

En quoi ça pose un problème? Dans le sens où on en met un parce qu'il faut en mettre un, parce que le système fonctionne avec un mot de passe, mais normalement, effectivement, on va vous donner quelque chose qui

n'est pas destiné à être votre mot de passe à long terme. Quel serait l'avantage? Parce que, là, obliger ça, ça veut dire légiférer, ça veut dire que le Québec se met dans une posture où il est le seul à... ou, en tout cas, parmi un groupe très sélect, là, parce que peut-être qu'il y a d'autres législations qui ont fait ça, je n'en ai pas eu connaissance, mais ça ne veut pas dire que ce n'est pas arrivé... où on irait là. Pour les entreprises, évidemment, ça amène des contraintes supplémentaires. Donc, est-ce que le jeu en vaut la chandelle?

M. Lemay-Leclerc (José) : Bien, on croit quand même que oui, parce qu'il y a vraiment beaucoup de piratages causés par ça, c'est assez connu, surtout au niveau des routeurs. Puis, quand on utilise le routeur, ça ne nous invite pas nécessairement à changer le mot de passe. Plusieurs peuvent mélanger le mot de passe administrateur du routeur et le mot de passe du réseau wifi. Donc, c'est quelque chose, quand même, qui peut être... c'est sûr que ça peut être difficile à implanter. En Californie, je sais qu'ils l'ont fait. Ça peut être implanté peut-être par phases, mais c'est quand même important, là, qu'au moins un routeur ne soit pas vendu sans configuration de sécurité, là, qu'on puisse le brancher directement et s'y connecter sans même... sans mot de passe, là.

M. Caire : Je m'excuse, est-ce que j'ai compris que la Californie avait légiféré dans ce sens-là?

M. Lemay-Leclerc (José) : Oui, oui.

M. Caire : Puis, en gros, elle dit quoi, la législation?

M. Lemay-Leclerc (José) : Elle interdit toute vente d'appareil qui n'a pas de configuration... J'ai mis le lien, là, dans mon mémoire. Bien, en fait, c'est... oui, ça interdit la vente d'appareils avec mot de passe par défaut — j'ai écrit «copieux», là — donc avec des mots de passe par défaut très simples, comme 1234, là, littéralement. Donc, c'est vraiment... ça ne permet que la vente d'appareils avec des mots de passe complexes ou semi-complexes.

M. Caire : Parce que, corrigez-moi si je me trompe, mais généralement, quand vous êtes l'acquéreur d'un appareil ou, en tout cas... qui nécessite l'utilisation d'un mot de passe, ça vient avec l'obligation de le modifier à la première utilisation, généralement.

M. Lemay-Leclerc (José) : Non. Ah! non, non, pas nécessairement.

M. Caire : Pas nécessairement, non?

M. Lemay-Leclerc (José) : Pas pour la plupart des routeurs.

M. Caire : O.K., là, on parle spécifiquement des routeurs?

M. Lemay-Leclerc (José) : Oui, bien, même les imprimantes, plusieurs appareils, souvent, ont un mot de passe ou aucun mot de passe.

M. Caire : Oui, mais, en même temps, ces appareils-là vont se connecter sur le réseau, puis généralement, si vous vous connectez sur le réseau, vous avez besoin d'utiliser le mot de passe réseau. Ça fait que ça revient un peu au même.

M. Lemay-Leclerc (José) : Oui, oui, mais c'est quand même prouvé, là, par plusieurs analyses qu'il y a eu beaucoup, beaucoup de piratages causés par ça.

M. Caire : O.K. Est-ce qu'il y a des évaluations qui ont été faites sur les bénéfices? Donc, est-ce qu'on a des chiffres qui nous disent que, par exemple, en Californie, il y a eu x nombre d'actes de piratages réussis, évidemment, de moins? Est-ce que c'est soutenu par une documentation, cette...

M. Lemay-Leclerc (José) : Oui, mais je ne l'ai pas avec moi, mais je pourrai vous la transmettre.

M. Caire : Non, non, c'est correct, on en prendra connaissance. Parce que je vous avoue que vous soulevez un point qui est intéressant puis qui suscite très certainement une réflexion. Donc, s'il y a une documentation qui peut nourrir la réflexion, oui, j'aimerais ça en prendre connaissance, là. Donc, vous dites que ça existe?

M. Lemay-Leclerc (José) : Oui, oui.

M. Caire : O.K. Votre dernière recommandation, bon, quand vous parlez de clarifier l'instance qui sera responsable de la gestion des appels d'offres, il faut comprendre que le ministère de la Cybersécurité et du Numérique... puis là ma réponse va peut-être être un peu plate, mais ça demeure le Conseil du trésor qui est le contrôleur financier de l'État. Ça demeure la Direction des marchés publics qui va réglementer et qui va s'assurer de la conformité des appels d'offres.

Puis il faut comprendre aussi, là, qu'au gouvernement du Québec, quand on va en appel d'offres, indépendamment de ce qui fait l'objet de l'appel d'offres, le processus est le même, l'autorité décisionnelle demeure la même. Donc, vous aurez remarqué que, dans le projet de loi, oui, le futur ministre de la Cybersécurité et du Numérique acquiert des pouvoirs qui sont actuellement assumés par la présidente du Conseil du trésor mais qui sont en lien, directement, avec son mandat. La gestion d'appel d'offres n'en fera pas partie. Par contre, vous remarquerez, dans le projet de loi, que le ministère de la Cybersécurité...

Le Président (M. Simard) : ...s'il vous plaît.

M. Caire : Oui, puis j'ai quelques secondes. Le ministère de la Cybersécurité et du Numérique devra émettre des avis sur les différents projets qui seront soumis au Conseil du trésor. Ce sera son mandat.

M. Lemay-Leclerc (José) : O.K. Donc, les appels d'offres sont comme publics, aussi, comme ils l'ont toujours été, là?

M. Caire : Oui, oui, tout à fait. Oui.

M. Lemay-Leclerc (José) : O.K. Parfait.

Le Président (M. Simard) : Alors, merci à vous, M. le ministre. Je cède maintenant la parole à la députée de Saint-Laurent.

Mme Rizqy : Merci beaucoup, M. le Président. Merci d'être présents avec nous. J'aimerais avoir vos suggestions pour que le gouvernement puisse accompagner les entreprises mais aussi les travailleurs à la maison, pour bien sécuriser le réseau. Ça serait quoi, en fait, les priorités du gouvernement pour faire cet accompagnement?

M. Lemay-Leclerc (José) : Oui, bien, c'est sûr que, comme là, ça a été suggéré ici, ça peut être un programme, là, de sensibilisation, des formations... bien là, je ne sais pas quel pourcentage de gens ça irait chercher, mais une bonne campagne de communication, oui, pourrait certainement sensibiliser beaucoup de gens. Et, bien, c'est sûr que nous, on avait quand même comme idée, là, d'aller voir jusqu'aux fournisseurs Internet. Mais oui, il y a vraiment beaucoup de choses à faire là-dessus parce que... Je vais juste prendre une gorgée d'eau.

Mme Rizqy : Pas de souci. L'importance de bien s'hydrater, particulièrement lorsque le temps frais revient.

M. Lemay-Leclerc (José) : Oui. Donc, parce qu'on le sait, les réseaux à la maison sont, pour la plupart, très peu sécurisés. Et bien, là, on le vit tous, on travaille de la maison, donc il y a vraiment un non-sens là-dessus. On ne veut pas non plus que les employeurs aillent jouer dans les configurations de nos réseaux de la maison. Donc, il faut vraiment que quelqu'un s'en occupe, là, c'est primordial. Est-ce que chaque résident doit s'occuper de son réseau informatique à la maison? Peut-être. Est-ce qu'on veut tous le faire? Est-ce qu'on peut tous le faire? C'est pour ça que c'est quand même une grande question, là.

Mme Rizqy : Je me permets de reculer un petit peu. Le télétravail, la grande majorité des Québécois apprécient, ça permet de gagner aussi du temps qui était, je vais le dire, perdu en transport, en déplacement. Par contre, ça demande aussi des ajustements à la maison. Du côté de l'employeur, ça veut aussi dire des économies, économie d'espace, économie aussi d'énergie, parce qu'évidemment une tour de bureau, est-ce que j'ai besoin de... je n'ai pas besoin d'avoir cinq étages, j'ai plutôt deux étages, je réduis non seulement mon espace, mais je réduis aussi ma facture d'électricité.

Je me mets à la place de l'employé. Lui, il a quand même des coûts associés à pouvoir faire ce virage et s'installer en télétravail à la maison, et ce n'est pas toutes les familles québécoises qui sont en mesure de s'équiper correctement. Est-ce qu'il devrait y avoir des mesures, puis là vous allez me voir venir, déformation professionnelle, fiscaliste en moi, des crédits d'impôt remboursables, pour peut-être aider les employés?

M. Lemay-Leclerc (José) : C'est sûr. C'est sûr qu'on accueillerait ce genre de gestes. Les travailleurs sont vraiment gagnants de mieux s'installer à la maison. Ça démarre aussi, évidemment, que l'employeur arrive avec une politique de télétravail et que, là, l'employé peut se préparer, savoir à long terme qu'est-ce que ça sera, les journées qu'il sera à la maison. Quand on sait qu'on va passer trois jours, deux, trois, quatre jours à la maison, huit heures par jour, bien, on a avantage à s'installer comme il faut, et là, oui, ça inclut des coûts, c'est sûr. On ne peut pas deviner que notre prochain employeur, s'il arrive quelque chose, va le permettre. Donc, ce n'est pas vraiment une installation qui appartient nécessairement à l'employé, là.

Mme Rizqy : Et, du côté de l'employeur, est-ce que lui aussi, de son côté... n'a-t-il pas une responsabilité financière envers son employé, lorsqu'il lui demande et requiert qu'il travaille à partir de la maison?

M. Lemay-Leclerc (José) : S'il a une responsabilité?

Mme Rizqy : Oui, financière, dans la mesure que certains employeurs vont dire : Nous, c'est terminé, ce n'est que du télétravail, donc c'est l'employé qui supporte à sa charge, par exemple, d'avoir un espace dédié à la maison, d'avoir une chaise ergonomique à la maison. À ce moment-là, l'employeur, lui... L'État peut faire sa part, mais il me semble qu'un employeur averti et responsable, si on transfère le fardeau d'espace de travail à la maison... il me semble qu'un employeur aussi devrait avoir une part à contribuer pour aider l'employé à être en mesure de faire du télétravail, lorsque c'est obligatoire, à la demande même de l'employeur.

M. Caza (Charles) : Dans le cas de l'employeur, parce que je représente, comme avocat en relations de travail, beaucoup d'employeurs... enfin, ma clientèle, c'est des employeurs...

• *(15 h 40)* •

Mme Rizqy : Je n'ai pas entendu. C'est une clientèle?

M. Caza (Charles) : Une clientèle d'employeurs. Je représente principalement des employeurs, donc je suis assez bien placé pour peut-être avoir un début de réponse à votre question. J'en parle un peu dans mon livre sur le télétravail, de cette question-là du fardeau, parce que, quand on force... Là, le cas de figure que vous donnez, c'est de forcer, et je le mets entre guillemets, l'employé à travailler chez lui ou une invitation forte à travailler chez lui. Dans ce cas-là...

Mme Rizqy : Exact.

M. Caza (Charles) : Oui, c'est exactement votre cas de figure. Dans ce cas-là, ça m'apparaît évident qu'un employeur doit contribuer, parce que, si c'est lui, c'est sa demande à lui, il lui dit : Bien, moi, pour une mesure d'économie, j'ai constaté, pendant la période du COVID, que je pouvais fonctionner au même régime, en faisant 100 % de profits mais en ayant quatre étages de vide, de la tour, et j'utilise seulement un étage, tout le monde à la maison, tout le monde travaille à la maison, dans ce cas-là, ça m'apparaît évident qu'il faut avoir une réflexion, que l'employeur doit payer. S'il force l'employé à travailler à la maison, il faut qu'il y ait une contribution de l'employeur, sur l'ordinateur, sur les mesures de sécurité. Mais là-dessus il y a un vide législatif, il n'y a pas de législation, au Québec, sur le télétravail. Tout le monde le sait, là, il n'y a rien, il y a un vide juridique. Un jour ou l'autre, il va falloir que le gouvernement ait une réflexion là-dessus.

Mme Rizqy : Bien, ça tombe bien parce que le jour est arrivé. Donc, durant la pandémie...

M. Caza (Charles) : Tant mieux, si le jour est arrivé.

Mme Rizqy : C'est pour ça que vous êtes présents avec nous. Mais c'est parce que, durant la pandémie, effectivement, le virage s'est opéré de façon obligatoire pour tout le monde. Mais maintenant il y a des acquis que plusieurs espèrent conserver, autant l'employeur que l'employé. Il y a des bénéfices, quand même, de part et d'autre, qui sont quand même intéressants.

Et là vous mettez un point tellement important, le vide juridique en question. Puis moi, j'aimerais ça aller un peu plus au fond des choses avec vous, parce que, justement, vous avez écrit des livres et faites des conférences, et j'imagine même que vous faites des conférences avec le Barreau sur différentes questions juridiques en droit du travail.

Maintenant, disons que la pandémie est terminée, juste pour les fins de notre dialogue entre nous deux et ceux qui nous écoutent — ils sont très attentifs, le ministre est aussi attentif — disons que la pandémie est terminée. À partir de maintenant, si on a un employeur, là, vraiment, qui décide que son modèle d'affaires, il n'y a plus d'urgence sanitaire, c'est son modèle d'affaires, c'est du télétravail, vous, c'est quoi, votre avis? Qui doit supporter cette charge, là, d'avoir... d'acheter un bureau, d'acheter une chaise ergonomique, d'acheter une imprimante, le papier et tout ça? Est-ce que ça devrait être à la charge de l'employeur?

M. Caza (Charles) : Bien, il y a... si on prend toujours le cas de figure dont vous mentionnez, la pandémie est terminée ou presque, disons ça de même...

Mme Rizqy : En cas de figure, elle est terminée. Pour le cas de figure, c'est terminé.

M. Caza (Charles) : Le cas de figure est terminé. C'est vrai que, statistiquement parlant, 76 % des personnes désirent avoir une forme de travail... de télétravail ou de travail qu'on appelle hybride, là, 76 % des gens désirent continuer de cette façon-là, à une ou plusieurs journées par semaine à la maison.

Bon, oui, si effectivement l'employeur consent à ça et l'employeur force... Parce que c'est toujours la question de savoir est-ce que c'est l'employé qui le désire ou si c'est l'employeur qui le force. Dans le cas de figure où l'employeur force l'employé à le faire, admettons, trois jours par semaine, c'est indéniable qu'il doit contribuer. C'est sûr, peu importe la façon dont il doit contribuer, sous forme de crédits ou sous forme de subvention, peu importe, mais, s'il force l'employé à avoir des biens chez lui, un ordinateur, une chaise, un bureau, bien, oui, il faut qu'il y ait une forme de contribution, c'est sûr.

Mme Rizqy : O.K. Et là, maintenant, on va faire l'exercice pour continuer. Parce que moi je me mets à la place de l'avocat qui représente l'entreprise. C'est quoi, forcer?

M. Caza (Charles) : Ce n'est pas forcer...

Mme Rizqy : C'est quoi, forcer? Parce que moi, si je suis l'avocate qui représente l'entreprise, je vais m'assurer de ne pas rentrer dans la catégorie «forcer». Alors, vous, ce serait quoi, les critères qu'on devrait porter une attention particulière pour déterminer si, à ce moment-là, l'entreprise force ou suggère fortement?

M. Caza (Charles) : Bien, «forcer» est peut-être un mot un peu fort, hein? On force peut-être le mot.

Mme Rizqy : On vous aime bien, vous. On va vous réinviter plus souvent.

M. Caza (Charles) : Dans le fond, on parle, en droit de travail, là... on parle d'obligation, on oblige quelqu'un à faire quelque chose, hein, c'est plus ça. Par exemple, si on oblige — on oublie le mot «forcer», on prend le mot «oblige» — oblige un employé à travailler chez lui trois jours par semaine ou même cinq jours par semaine, c'est une obligation de le faire...

Mme Rizqy : Ah! bien, ça, c'est un cas assez patent. Moi, je veux arriver dans la zone grise. Donc, par exemple... là, je ne veux pas vous mettre des mots dans la bouche, c'est quand même vous, notre invité du jour. Alors, disons que, par exemple, vous avez une entreprise qui n'offre pas à un employé un bureau attitré. Tu sais, je vous donne certaines conditions, là, qui pourraient faire en sorte que l'employé comprendrait qu'il est très fortement appelé à rester à la maison : donc, pas de bureau attitré, pas de ligne de téléphone attitrée, qu'on lui dit d'apporter un ordinateur, au fond, qui ne sera pas à une place fixe, mais ça sera plutôt un ordinateur comme j'ai présentement, un ordinateur portable. Veux veux pas, ce n'est pas un lieu de travail fixe comme qu'on connaissait traditionnellement, là. Ça, est-ce que ça pourrait être considéré comme une suggestion forte de rester à la maison? Là, j'ai comme posé la question qui tue, on dirait.

M. Caza (Charles) : C'est peut-être plus une invitation, là, dans ce cas-là.

Mme Rizqy : C'est... Comment?

M. Caza (Charles) : C'est peut-être plus une invitation à travailler à la maison. Ce n'est peut-être pas nécessairement une obligation de le faire, c'est peut-être une invitation. Mais de plus en plus de personnes, d'employeurs, et de syndicats, et de groupes de salariés, des salariés individuels, ont des ententes, des politiques qui prévoient le partage des coûts. Il y en a de plus en plus, là. Évidemment, il n'y en avait pas avant le mois de mars 2020, il n'y avait rien de ça, mais maintenant il y a des politiques à l'interne, il y a des politiques sur le télétravail, de plus en plus.

Le Président (M. Simard) : Très bien. Je crois comprendre, chère collègue, que votre partenaire souhaiterait peut-être intervenir, à ce stade-ci. Avec le consentement, on va pouvoir déborder un peu afin que vous puissiez intervenir.

Des voix : Consentement.

Mme Nichols : Consentement? Merci, M. le Président. C'est très apprécié. Mais c'était très pertinent, là, les propos de ma collègue. Donc, merci. Merci. Je vous salue, les deux. Je connais Me Caza. Donc, bonjour, Me Caza. Dans le monde municipal, là, on a déjà travaillé ensemble, Me Caza a déjà représenté...

M. Caza (Charles) : Oui, dans une vie antérieure. Vous, dans une vie antérieure.

Mme Nichols : Oui, dans une vie antérieure. Bien là, moi, je ne suis pas blanche, ça fait que...

M. Caza (Charles) : Moi non plus. Moi non plus. Je suis gris foncé.

Mme Nichols : Mais, tout à l'heure, M. Lemay-Leclerc, il nous disait, entre autres, que les experts en sécurité devaient avoir le dernier mot dans la production... dans la protection et la production des infrastructures numériques logicielles. Évidemment, là, ça va de soi, là. Mais moi, ce qui m'intéressait, c'est l'aspect sécurité. Est-ce qu'il y avait des recommandations à cet effet-là, là, au niveau sécurité des tests périodiques qu'on doit faire? Est-ce qu'il y a des recommandations?

M. Lemay-Leclerc (José) : Oui. Bien, c'est sûr qu'autant la sécurité... tu sais, ce qu'on dit souvent, c'est que ça prend des bonnes routines, il faut qu'il y ait des analyses de faites, des rapports. Souvent, tout ça s'automatise au minimum, au maximum, mais ça peut être, évidemment, automatisé. Il faut aller voir un peu, là, les journaux, les logs, qu'on appelle. Mais oui, c'est important que la cybersécurité ait un peu le dernier mot à dire, là, sur le numérique, là. C'est vraiment essentiel.

Parce que, s'il arrive quelque chose... Puis il en arrive, des erreurs, c'est souvent humain. J'ai été témoin, moi-même, là, d'erreurs. Puis souvent, les piratages... bien, pas souvent, mais quand même, quelquefois, les piratages sont causés

par des erreurs, là, des configurations, des choses comme ça. Donc, il faut que les spécialistes en cybersécurité, vraiment, n'aient aucune contrainte à... pas dénoncer, mais vraiment à dire qu'est-ce qu'ils ont trouvé comme problèmes, même si les problèmes ont été causés par leur collègue, là, dans ce cas-ci, littéralement.

Mme Nichols : Parfait. Je voulais juste confirmer que c'était nécessaire, qu'il fallait que ce soit là puis que ce soit obligatoire. Donc, merci de votre réponse. Merci, M. le Président, pour votre...

Le Président (M. Simard) : Merci, chère collègue. Merci. Alors, bien, M. Lemay-Leclerc ainsi que M. Caza, merci beaucoup de votre présence fort éclairante aujourd'hui, votre témoignage fort apprécié. Nous vous remercions à nouveau.

Sur ce, on va suspendre momentanément, le temps de faire place à nos prochains invités.

(Suspension de la séance à 15 h 49)

(Reprise à 16 h 02)

Le Président (M. Simard) : Alors, chers collègues, heureux de vous retrouver tous et toutes, des deux côtés de cette chambre. Nous sommes en présence de M. Steven Lachance, expert en cybersécurité. Monsieur, bienvenue parmi nous. Vous êtes le dernier mais non le moindre de cette importante consultation. Merci de vous joindre à nous. Vous disposez d'une période de 10 minutes.

M. Steven Lachance

M. Lachance (Steven) : Merci, merci. Alors, bonjour, tout le monde. Cher ministre et chers députés, merci de me faire l'honneur de m'inviter à m'entretenir avec vous aujourd'hui. Steven Lachance, je suis programmeur et entrepreneur en technologies, essentiellement, depuis l'âge de 15 ans, militant de longue date en tout ce qui gravite autour des enjeux de sécurité des données personnelles et vie privée.

Dans la dernière année, j'ai fréquemment été amené à contribuer à titre d'analyste en technologie et cybersécurité dans différents médias, dont TVA, Radio-Canada, CBC, CTV, etc. Et j'aimerais aujourd'hui débuter en faisant un survol, là, de deux des sujets où j'ai été amené, là, à contribuer davantage dans la dernière année.

Le premier, c'est celui du passeport vaccinal. Permettez-moi, là, de passer en rafale, là, une analyse, là, du bon et du mauvais de ce dossier-là, question non plus de mettre la table, là, pour ce qui suivra. En commençant avec le bon, bien, ce que Québec a fait, c'est qu'on a retenu, là, la meilleure technologie existante, un standard international, là, «open source». On a donné ensuite le développement de ça à une PME d'ici. On a fait preuve d'un leadership au Canada. On a été les premiers au Canada, et ensuite toutes les provinces ont suivi. Ça aura permis une interopérabilité entre ici et ailleurs, maintenant, avec tout le monde puisque d'autres États américains ont la même technologie. Et le système reposait, là, sur la minimisation des données. Donc, il n'y a pas de base de données centralisée, et donc il n'y a pas de suivi des déplacements possible, et il n'y a rien à voler. Donc, ça, c'est des très bonnes choses.

Par contre, si on regarde au niveau des moins bonnes, selon moi, il y a eu un certain manque de transparence dans le processus décisionnel, là, qui s'est fait un peu, là, derrière des portes closes. Le développement des applications, lui, du portail et l'hébergement, tout ça s'est fait par la même firme externe privée. Le sort des données est laissé entre les mains de cette firme privée là. Le code source de ce qui a été développé au Québec est resté fermé, n'a pas été partagé. Conséquemment, bien, il y a eu un dédoublement entre chaque province et aucun réel partage, là, à l'international. C'était le premier dossier.

Le deuxième, celui de Terre-Neuve, le cas de la cyberattaque contre le ministère de la Santé de Terre-Neuve qui est survenue, là, il y a quelque chose comme autour d'un mois, que plusieurs appellent la pire cyberattaque de l'histoire du Canada... C'est une fuite de données extrêmement sensibles dans les hôpitaux, là, de patients et d'employés allant jusqu'à les 14 dernières années, des bases de données mal protégées qui étaient dans une suite logicielle, là, qui est pourtant utilisée à travers, là... dans plusieurs provinces canadiennes.

Donc, ce qu'on constate dans tout ça, malheureusement, c'est que les hôpitaux et les autres ministères, etc., sont condamnés à jouer constamment une espèce de jeu, là, de la taupe à subir les attaques informatiques dans une sorte de spirale sans fin.

Ce qu'on constate également, ce que je constate, c'est que, M. le ministre, vous avez devant vous une espèce de mission impossible. Avec la rapidité de la multiplication des attaques, de la mobilité de la main-d'oeuvre en contexte de télétravail, de la concurrence des salaires dans le privé pour le personnel, combinés avec la rareté de l'expertise, par-dessus ça, vous devez composer avec le fait que, bon, les gouvernements, les ministères sont des structures relativement rigides, qui font moins rêver les jeunes têtes que certains autres acteurs, qui ont des budgets restreints ou limités et dont le pouls est relativement lent pour l'industrie. Vous avez la mission de rendre une espèce de dinosaure et de le faire s'adapter à un monde en rapide évolution.

En d'autres mots, M. Caire, vous avez... vous êtes en désavantage systémique. Ce que vous aurez à mettre sur pied, c'est le plus agile et le plus souple de tous les ministères. Et, dans le contexte, il y a deux clichés qui valent la peine d'être gardés en tête.

Le premier, c'est le classique : vaut mieux prévenir, plutôt que guérir. Le deuxième, c'est la fameuse citation de Wayne Gretzky, qui disait : Patinez où la rondelle s'en va, pas là où elle est déjà. C'est cliché, mais ça a le mérite

d'être vrai, surtout dans le contexte auquel on fait face présentement. Pour sortir du cercle vicieux dans lequel on est, il va falloir faire preuve d'anticipation et d'adaptabilité.

Une des grandes avenues de solutions, là, pour multiplier notre retour sur investissement, c'est de mettre à profit, là, deux éléments clés, c'est l'«open source» et la collaboration internationale. Donc, en formant une grande coalition internationale, là, de partage de solutions, autant en cybersécurité qu'en développement logiciel, on multiplie les ressources et on divise les coûts. Donc, c'est une pierre deux, trois, quatre coups. Plus on développe en code ouvert, plus on partage nos solutions, plus il y a de cerveaux qui s'impliquent, plus les solutions sont étudiées, utilisées, plus on permet la contribution ad hoc, plus les solutions s'améliorent, s'adaptent et s'actualisent.

Plutôt que d'opérer dans une logique constamment en vase clos, plus classique, on pourrait très bien s'allier avec, exemple, l'Ontario, New York, la Finlande, qui que ce soit, et unir nos ressources pour combler nos besoins communs. Collaborer à l'international, partager nos solutions comme ça, ça ne nous rend pas davantage dépendants sur les autres. En fait, ça nous rend davantage indépendants, et les développeurs québécois pourraient contribuer non seulement aux outils utilisés localement, mais aussi internationalement. Et ça, c'est le genre de choses, je pense, qui est extrêmement stimulant pour les communautés de développeurs qui contribueraient grandement à la rétention, à l'attraction, à la rétention de la main-d'oeuvre. Libérer nos systèmes en «open source», ça ne coûte essentiellement rien. C'est une approche qui mettrait à profit l'expertise des experts d'ici et d'ailleurs, et plusieurs outils, là, pourraient aussi d'ailleurs être réutilisés au municipal.

• *(16 h 10)* •

Toujours sur le plan financier, on doit minimiser les dépenses extérieures, on doit chercher à minimiser le plus possible les dépenses extérieures, le moins de dollars possible qui doivent sortir du Québec. La pandémie a fait réaliser, là, l'importance du local à bien des gens, cultiver notre autonomie locale via les investissements locaux, appliquer également le principe d'argent public égal code public partout où possible. Ce n'est pas possible dans tous les cas. Par contre, c'est un principe qu'on doit garder en tête ou qu'on doit chercher à appliquer davantage. Mettre à profit les PME aussi, abaisser les barrières à l'entrée pour favoriser leur participation et pas celle seulement, là, des grands gérants étrangers qu'on connaît tous. C'est une façon assurée aussi de stimuler l'innovation québécoise.

Et, M. Caire, vous avez brièvement mentionné en audience hier l'idée d'appel aux solutions publiques. Je pense qu'il y a là une extraordinaire possibilité, là, à sommer ou à explorer, une espèce, là, de place de marché gouvernemental, de services informatiques gouvernementaux, optimisés pour faire travailler les entreprises innovantes d'ici sur les innombrables problèmes de nature publique. Je pense que ça vaut la peine d'être exploré davantage.

Ensuite, au-delà de l'aspect plus strictement financier, je pense qu'il doit y avoir un certain changement de culture au gouvernement, entre autres, sur la question de l'horizon, là, technologique. C'est que les choix technologiques qu'on fait au gouvernement ont... affectent directement la rétention de la main-d'oeuvre, et non seulement les budgets, sur les 10 années à venir.

Oui, il faut minimiser, évidemment, bon, les choses comme les coûts de durée de vie, etc., mais il faut aussi maximiser le bien-être des développeurs. Et ça, le privé l'a compris. Les choix technologiques affectent ça grandement puis sont... vont être un facteur très important pour attirer et retenir les développeurs.

Ensuite, la sécurité doit commencer à faire partie de l'ADN du gouvernement, je dirais, tout autant, là, qu'exemple, la langue française. Bien, ça doit devenir un réflexe organisationnel à travers l'ensemble des ministères et toutes les décisions et les choix informatiques doivent être prises avec la sécurité en tête.

Il faut également, malheureusement, être en constante préparation pour toutes formes d'hostilités inattendues. Les menaces ne sont pas seulement, là, russes ou chinoises comme dans les films, là. Elles peuvent aussi être québécoises, canadiennes ou américaines, elles peuvent venir de nos alliés, sachant qu'Obama espionnait Angela Merkel, sachant que les Britanniques qui ont espionné les communications de leurs alliés au sommet du G20 à Londres... Sachant que Trudeau père espionnait René Lévesque, est-ce que Trudeau fils ou ses successeurs pourraient s'intéresser, par exemple, à François Legault, à Gabriel Nadeau-Dubois ou à tout autre successeur? Sachant qu'Obama espionnait Petrobras, la pétrolière nationale brésilienne, à des fins commerciales pour faire bénéficier les États-Unis dans leurs négociations énergétiques commerciales avec le Brésil, est-ce que les Américains, présentement, pourraient s'intéresser aux communications de Sophie Brochu?

Ce qui nous amène à ce que... certains angles morts, je pense. Dans le projet de loi, il y a certaines questions qui demeurent pour moi. Est-ce que ce nouveau ministère de la Cybersécurité, est-ce que c'est ce ministère-là qui va être chargé de protéger les communications du premier ministre, du Conseil des ministres, de l'Assemblée nationale, de la présidente d'Hydro-Québec? Et qu'est-ce qui en est d'au-delà du gouvernement? Le projet de loi se limite aux ministères puis aux agences gouvernementales, mais, dans un sens, c'est comme un peu comme si le ministère de la Santé soignait seulement les ministères, les entreprises. Les citoyens sont laissés de côté. On peut comprendre que ça serait un grand élargissement, là, du mandat, mais ça demeure néanmoins problématique.

Et un autre angle mort, je crois, c'est les municipalités. Elles ont les mêmes enjeux de cybersécurité, les mêmes enjeux de systèmes informatiques, mais pas les mêmes ressources. Elles peuvent et doivent apprendre les mêmes bonnes pratiques. Elles ont besoin d'accompagnement, que ce soit formation, prévention, inspection au-delà du ministère, là, en tant aussi que courtier infonuagique, là, tel qu'il est prévu dans le projet de loi, ce qui touche essentiellement, là, selon ma compréhension, juste les plus gros, là, Microsoft, là, de ce monde. Une espèce de courtier des PME technologiques mettrait à profit, là, l'expertise locale de nos entreprises et pourrait l'étendre aux municipalités, donc une place de marché public pour services informatiques publics. Si le gouvernement du Québec est protégé, mais que la ville de Montréal ne l'est pas, ou la ville de Québec, on n'est pas particulièrement plus avancés.

Le Président (M. Simard) : En conclusion.

M. Lachance (Steven) : Oui, en conclusion, alors je soulevais simplement les points... Les conseils de ville, les psychologues, les avocats, les comptables, ce sont tous des points névralgiques qu'on doit garder en tête pour la protection long terme du Québec en matière de cybersécurité. Sur ce, je vous cède la parole, et ça me fera plaisir de répondre à vos questions.

Le Président (M. Simard) : Merci à vous, M. Lachance. Pour des fins procédurales, notre secrétariat nous informe que nous avons légèrement dépassé le temps prévu à l'horaire, donc nous aurions besoin de votre consentement éventuellement pour poursuivre au-delà de l'heure prévue. Il y aurait consentement. Très bien.

Alors, à ce stade-ci, deux collègues souhaitaient intervenir, la députée de Vaudreuil, bien sûr, et le député de Vanier. Alors, M. le député de Vanier, souhaitiez-vous intervenir?

M. Asselin : Bonjour, M. Lachance. Je trouve ça intéressant, votre présentation, puis, en même temps, c'est plutôt rare que, dans l'enceinte de l'Assnat, Wayne Gretzky est cité. Alors, vous avez touché la formule.

Vous avez parlé de changement de culture. J'aimerais ça que vous élaboriez un petit peu plus sur le côté changement de culture en rapport avec le projet de loi n° 6. Qu'est-ce que vous voyez qui compte... Comment vous voyez qu'on pourrait insérer ça dans le projet de loi?

Le Président (M. Simard) : M. Lachance.

M. Lachance (Steven) : Bien, je ne sais pas comment ça pourrait être inséré dans un article dans le projet de loi en tant que tel. Par contre, ce qui est certain, c'est que, sur le long terme, hein, si on essaie d'anticiper, là, si on regarde les 10 années à venir, de quoi est-ce qu'on a de besoin dans la fonction publique québécoise, on a... un des grands, grands problèmes, et ça a été soulevé, là, par nombre d'intervenants précédents, c'est au niveau de la main-d'oeuvre, comment est-ce qu'on va attirer des gens, du personnel, des experts qualifiés. Et il va y avoir... Je pense que l'environnement de travail, l'environnement technologique, les choix technologiques qu'on fait, à qui on donne les mandats les plus intéressants, de quelle façon on opère à l'intérieur des équipes de développement, je pense que c'est susceptible de faire une différence énorme sur la capacité du gouvernement à attirer le meilleur personnel.

Et, ensuite de ça, l'autre chose, quand je disais un changement de culture, la sécurité doit prendre une beaucoup plus grande place dans les réflexions, non seulement au ministère de la Cybersécurité, mais à travers tous les ministères. Ça doit devenir un réflexe organisationnel où est-ce que tout est pensé à travers cette lentille-là pour s'assurer qu'on ne fasse pas... qu'il ne nous arrive pas qu'est-ce qui vient d'arriver à Terre-Neuve et qu'il ne nous arrive pas possiblement pire.

M. Asselin : Je vous remercie de votre témoignage. Je déduis entre les lignes que vous êtes enthousiaste par rapport aux changements qu'apporte le projet de loi n° 6. Est-ce que je comprends bien votre intervention?

M. Lachance (Steven) : Enthousiaste, c'est que c'est certainement... Le fait que ces ressources-là soient centralisées au sein d'un même ministère, je pense que ça va être bénéfique pour l'État québécois à long terme, c'est certain. Ça démontre un certain sérieux. Ça va éviter, j'en suis sûr, les dédoublements, là, de personnel, ou de ressources, ou de dépenses, ou etc. Ça va faire une espèce de guichet unique, là, pour composer avec les enjeux informatiques. Donc, à prime abord, oui, effectivement, je salue l'apparition de ce nouveau ministère.

Le Président (M. Simard) : Merci à vous. Je cède maintenant la parole au député de Saint-Jérôme.

M. Chassin : Merci, M. le Président. M. Lachance, en fait, il y a une question qui m'est venue à l'esprit, là, un peu spontanément quand vous avez parlé de la sécurité, par exemple, des communications du premier ministre ou de la présidente d'Hydro-Québec. Est-ce que... Puis là je mise vraiment sur votre expertise, je ne suis absolument pas expert dans le domaine.

Est-ce que vous avez une compréhension, par exemple, d'avantages que pourrait avoir le fait que ce soit ce ministère qui s'occupe de la sécurisation des communications par rapport, par exemple, à la sécurité du Québec ou à des corps policiers?

M. Lachance (Steven) : Pouvez-vous préciser votre question?

• *(16 h 20)* •

M. Chassin : Quand vous disiez, par exemple, que, bon, on a déjà vu de l'espionnage entre dirigeants d'État, même pour des fins commerciales avec les États-Unis qui espionnaient Petrobras... Donc, dans ce contexte-là, vous posiez la question : Est-ce que le nouveau ministère en Cybersécurité s'occuperait de s'assurer de la sécurisation des communications pour, par exemple, le premier ministre ou la P.D.G. d'Hydro-Québec? Est-ce que vous avez une compréhension de quels seraient, mettons, disons, les avantages et les inconvénients que ce soit ce ministère-là qui s'en occupe plutôt qu'un corps policier?

M. Lachance (Steven) : Je n'ai pas de... je ne suis certainement pas spécialiste de la fonction publique ou du fonctionnement interne des ministères, etc. Je soulève la question parce que, que ce soit le mandat de ce nouveau

ministère là ou pas, ça doit être le mandat de quelqu'un et ça doit être pris extrêmement au sérieux. Et ça s'applique à beaucoup, beaucoup de gens, de personnes, d'employés, d'agences gouvernementales. Il y a énormément... il y a un énorme volume de communications à sécuriser et ça doit faire davantage partie de notre culture que de protéger nos communications et de ne pas... d'arrêter d'être négligent, des fois, sur ces questions-là.

M. Chassin : Je comprends. Donc, autrement dit, qu'on s'assure que la responsabilité soit donnée à quelqu'un. À la limite, le ministère peut s'assurer que quelqu'un le fasse de façon compétente, mais n'a pas à le faire lui-même.

M. Lachance (Steven) : Non, effectivement. Ça pourrait être au ministère de la Cybersécurité, ça pourrait être aussi à la Sécurité publique, en autant que ça soit à quelqu'un.

Le Président (M. Simard) : Merci à vous, cher collègue. Ça vous va? Je cède maintenant la parole à la députée de Vaudreuil qui va conclure cet échange.

Mme Nichols : Oui, certainement, comme je fais depuis les derniers jours.

Le Président (M. Simard) : Bien oui. Avec brio, soit dit en passant.

Mme Nichols : Merci, M. le Président, je l'apprécie énormément. Deux petites questions. Ma première question va peut-être suivre dans la même logique, là, que le député de Saint-Jérôme. On parlait, là, d'espionnage de la P.D.G., entre autres, d'Hydro-Québec, même du premier ministre. Je me demandais, c'est quoi, les références... en fait, sur quoi vous vous basez, c'est quoi, les références qui vous amènent à dire qu'il y a de l'espionnage au niveau de la P.D.G. d'Hydro-Québec ou du premier ministre?

M. Lachance (Steven) : Bon, attention, je n'ai pas affirmé qu'il y avait de l'espionnage après de la P.D.G. ou du premier ministre. J'ai soulevé des questions, j'ai nommé des exemples documentés historiques d'espionnage entre alliés, que ce soit entre différents pays ou pour des raisons commerciales, etc. Et je crois que ça doit être pris en considération, on doit se structurer, nos organisations, pour se protéger, se protéger de ce qu'on perçoit comme étant des ennemis géopolitiques, mais aussi se protéger de menaces potentiellement internes, ou à même le pays, ou de nos alliés, etc. Je ne suggère en rien que Sophie Brochu est présentement espionnée, là.

Mme Nichols : Mais vous avez fait aussi référence, là, à des entités, là, névralgiques, vous avez... puis ça a sonné tout de suite à mes oreilles parce que vous avez parlé d'un conseil... du conseil municipal, là, qui peuvent être, justement, des points névralgiques. Vous expliquez ça comment? Je ne comprends juste pas, là, le lien comment un conseil municipal pourrait devenir un point névralgique.

M. Lachance (Steven) : J'ai nommé un exemple, une liste, le conseil de ville, les psychologues, des avocats, des comptables, etc. C'est que c'est des endroits ou c'est des organismes ou organisations dans la société qui prennent des décisions extrêmement importantes et qui... dont les communications peuvent intéresser bien des gens. Les conseils de ville, peut-être qu'une petite municipalité nous paraît n'intéresser personne. Par contre, des conseils de ville de plus grandes villes, ça peut avoir... les communications de ces gens-là peuvent intéresser définitivement plusieurs, et ça doit être pris en compte. Le ministre Caire parlait du ministère de la Cybersécurité comme étant quelque chose qui allait mettre un périmètre de sécurité autour de l'État québécois et des agences gouvernementales. Je crois que ça devrait, philosophiquement, s'étendre aux municipalités aussi.

Mme Nichols : En effet, le ministre Caire, là, nous a donné beaucoup d'informations, là, pendant ces auditions. Croyez-vous que n'importe qui pourrait, entre autres, là, que n'importe qui peut être employé dans le domaine de la cybersécurité? Question simple comme ça. Est-ce que ça prend des qualifications en particulier pour être un expert ou être qualifié en cybersécurité? N'importe qui pourrait être un employé dans ce domaine-là? C'est une question. Ce n'est pas une affirmation, c'est une question.

M. Lachance (Steven) : Je pense que, comme dans tous les domaines spécialisés d'expertise de pointe, ça demande une certaine expérience. C'est un... je ne pense pas, non, qu'on puisse engager n'importe qui. Ce n'est pas, par contre, un domaine où est-ce qu'il y a une espèce d'ordre professionnel, où est-ce que la formation académique est particulièrement nécessaire. Les meilleurs hackeurs n'ont pas appris à hacker à l'université, là, et donc...

Mme Nichols : Quelles compétences devrait avoir la relève, parce qu'il va y avoir une relève sûrement ou il va y avoir... quelles compétences on devrait rechercher, justement, entre autres, pour assurer la sécurité du gouvernement du Québec?

M. Lachance (Steven) : La débrouillardise informatique...

Mme Nichols : Bien, ça, ce n'est pas rassurant, parce que moi, je me débrouille, mais je ne suis vraiment pas une experte, là.

M. Lachance (Steven) : Bon, écoutez, c'est un peu comme des développeurs de logiciels, hein, ça prend une certaine maîtrise des concepts logiciels, des concepts réseautiques, aussi une certaine curiosité géopolitique, et historique, et philosophique.

Mme Nichols : Très bien. Je n'ai pas d'autre question. Merci, M. le Président.

Le Président (M. Simard) : Merci à vous, chers collègues. Alors, M. Lachance, merci beaucoup d'avoir participé à nos travaux. Ce fut fort apprécié.

Mémoires déposés

Sur ce, je dépose les mémoires des organismes non entendus. Et ne partez pas tout de suite, nous allons suspendre momentanément nos travaux afin de revenir avec une motion sur laquelle... dont je vais vous parler à l'instant. Alors, nous suspendons.

(Suspension de la séance à 16 h 28)

(Reprise à 16 h 29)

Le Président (M. Simard) : Alors, chers collègues, voilà, avant de mettre fin à la séance, comme vous le savez, la prorogation de la première session de la 42e législature a mis fin à tous les ordres et à tous les mandats qui avaient été adoptés par notre commission. En conséquence, nous devons procéder de nouveau à la mise aux voix d'une motion, celle qui vise à constituer un comité directeur. Je comprends qu'il y a consentement afin de procéder à la mise aux voix de cette motion pendant l'actuelle séance? Il y a consentement?

Des voix : Consentement.

Le Président (M. Simard) : Merci, chers collègues. Alors, afin de créer de nouveau le comité directeur de la commission, je vous propose la motion suivante :

«Que la Commission des finances publiques, conformément à l'article 4 des règles de fonctionnement, constitue un comité directeur composé du président, de la vice-présidente ainsi que la secrétaire.»

Est-ce que cette motion est adoptée?

Des voix : Adopté.

Le Président (M. Simard) : Adopté. Conséquemment, chers amis, merci beaucoup pour votre précieuse collaboration, ce fut là de belles auditions.

Et nous ajournons nos travaux sine die. À bientôt.

(Fin de la séance à 16 h 30)